BÁO CÁO BÀI THỰC HÀNH SỐ 7

**PHÂN TÍCH MỘT SỐ KỸ THUẬT THĂM DÒ MẠNG**

***Họ và tên sinh viên: Hoàng Văn Hiếu***

***MSSV: 1050080179***

***Yêu cầu kết quả thực hành:***

Kết quả bỏ vào file word có tên theo định dạng HoangVănHieu\_1050080179\_Lab07

* Báo cáo kết quả thực hành
* File bắt lưu lượng trên các máy do thám của mỗi kịch bản. Kích thước mỗi file không quá 5MB.

**KẾT QUẢ THỰC HÀNH**

1. **Phân tích một số kỹ thuật quét cổng ứng dụng của nmap**
   1. **Kịch bản 1: Quet thăm dò mạng**

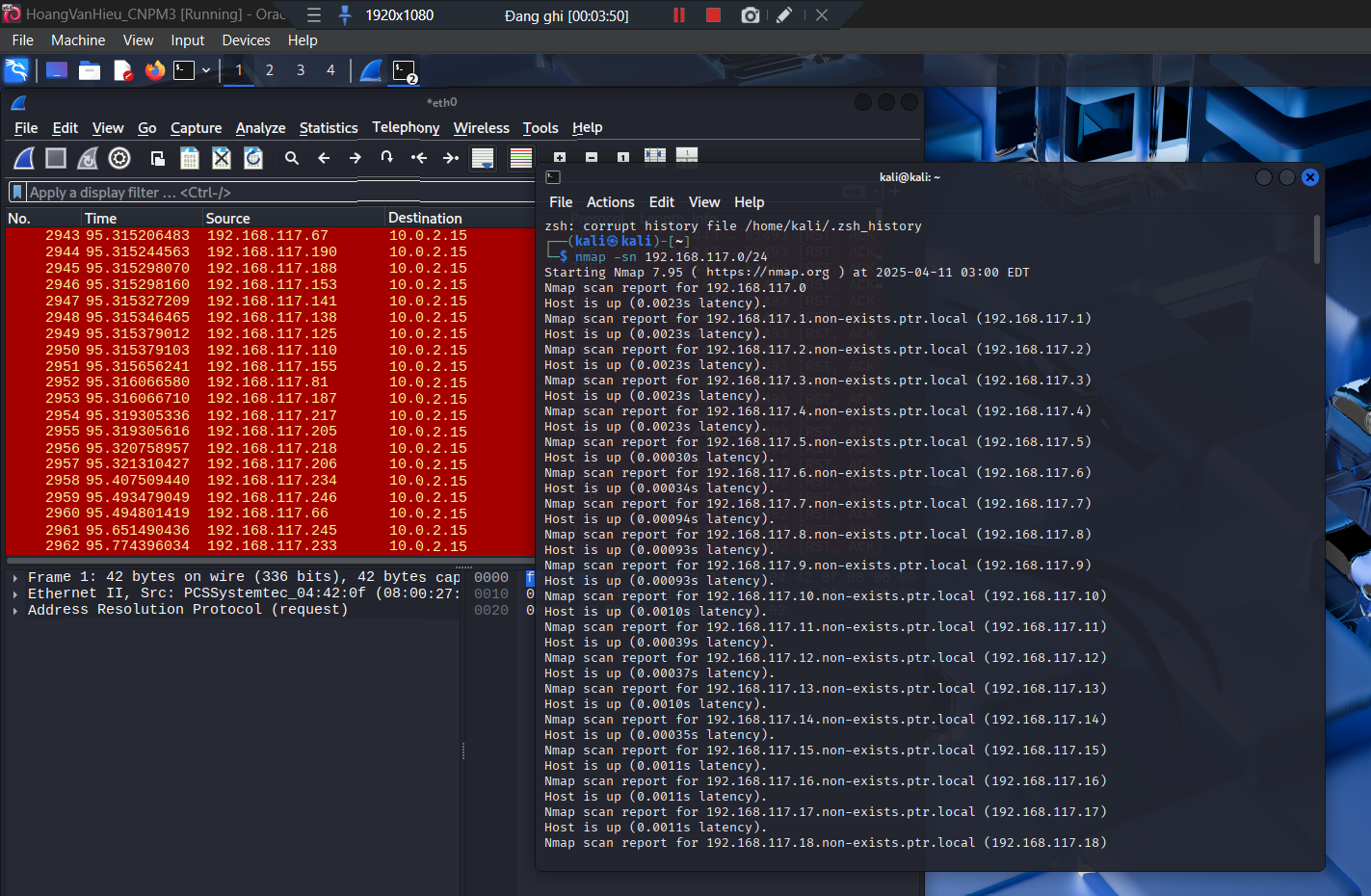
* Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm

- **Bước 1:** Truy cập máy ảo Attack

- **Bước 2:** Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin. - **Bước 3:** Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

nmap -sn 192.168.117.0/24

- **Bước 4:** Sau khi nmap thực hiện xong quá trình quét mạng, ta có thể thấy kết quả tương tự như sau:

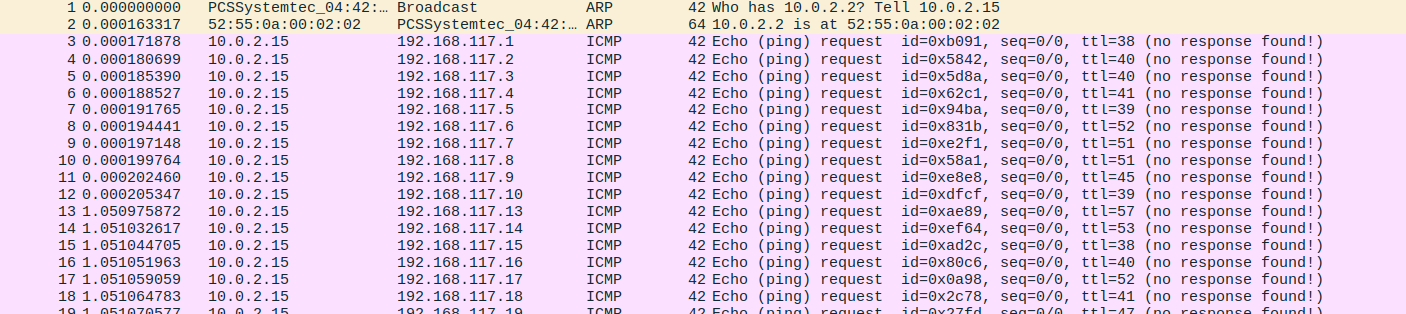


- Bước 5 : dừng bắt gói tin trong Wireshark.

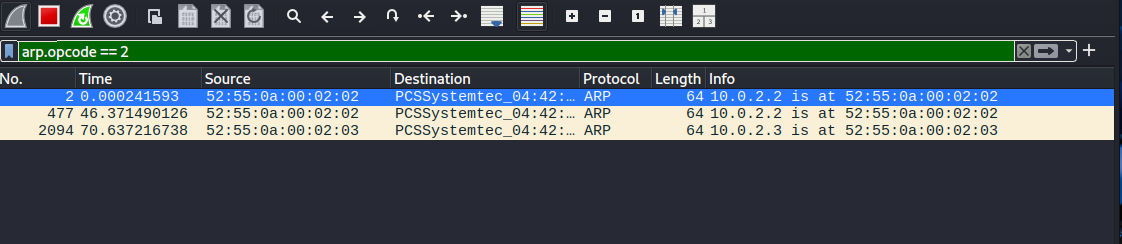
* **Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm**

***Phân tích lưu lượng :***

* Quan sát màn hình bắt gói tin trên wireshark, ta thấy rằng máy tấn công đang gửi đi các gói tin ARP Request để tìm kiếm địa chỉ .



* Trên cửa sổ của Wireshark, sử dụng giá trị **arp.opcode == 2** cho bộ lọc, chúng ta có thể thấy các gói tin ARP Reply được gửi lại từ các nút mạng đang hoạt động đã quan sát thấy ở trong kết quả quét mạng bằng công cụ nmap.



=> Kết quả: như vậy trong kịch bản thực hiện 1, Nmap đã sử dụng kỹ thuật ARP Ping Scan để phát hiện các nút mạng hoạt động trong mạng.

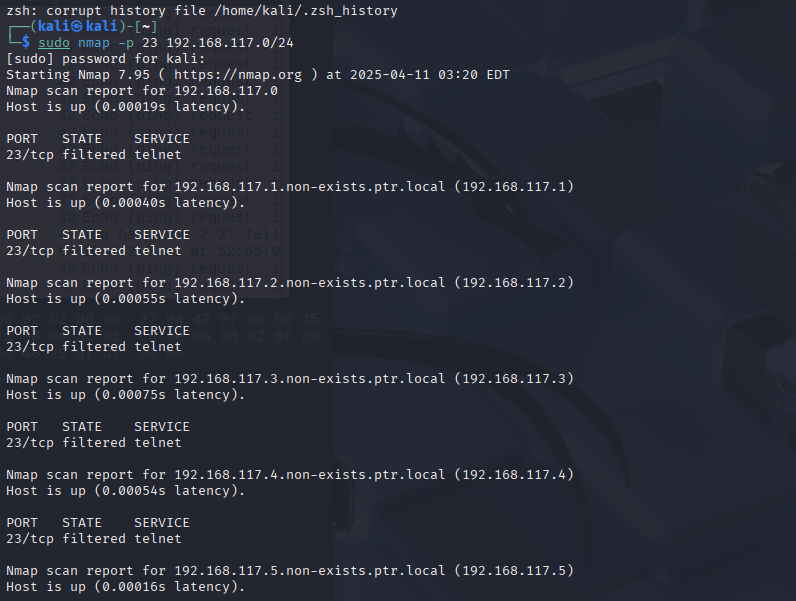
* 1. **Kịch bản 2 : Quet thăm dò dịch vụ**
* Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm
* Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm

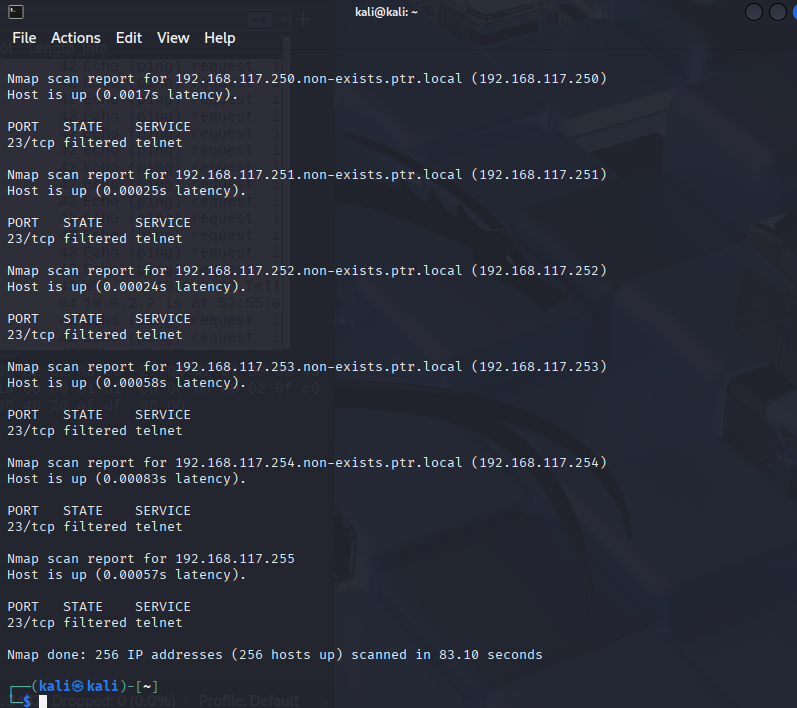
- **Bước 1:** Truy cập máy ảo Attack

- **Bước 2:** Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin. - **Bước 3:** Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

**sudo nmap -p 23 192.168.117.0/24**

- **Bước 4:** Sau khi nmap thực hiện xong quá trình quét thăm dò, ta có thể thấy có các nút mạng 192.168.117.13 và 192.168.117.10 có trạng thái cổng dịch vụ 23 là open. Như vậy, ta có thể phán đoán rằng các máy này đang cung cấp dịch vụ Telnet.

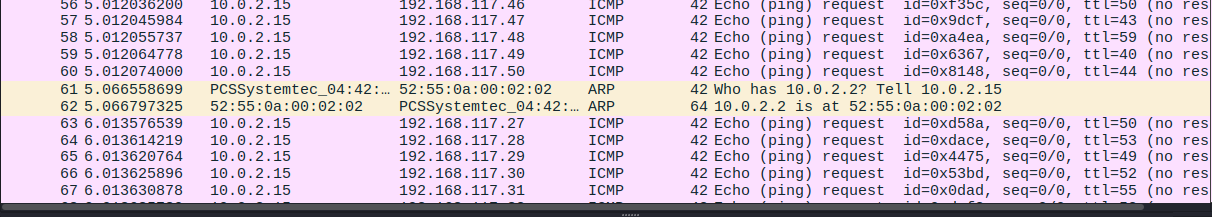
**

**

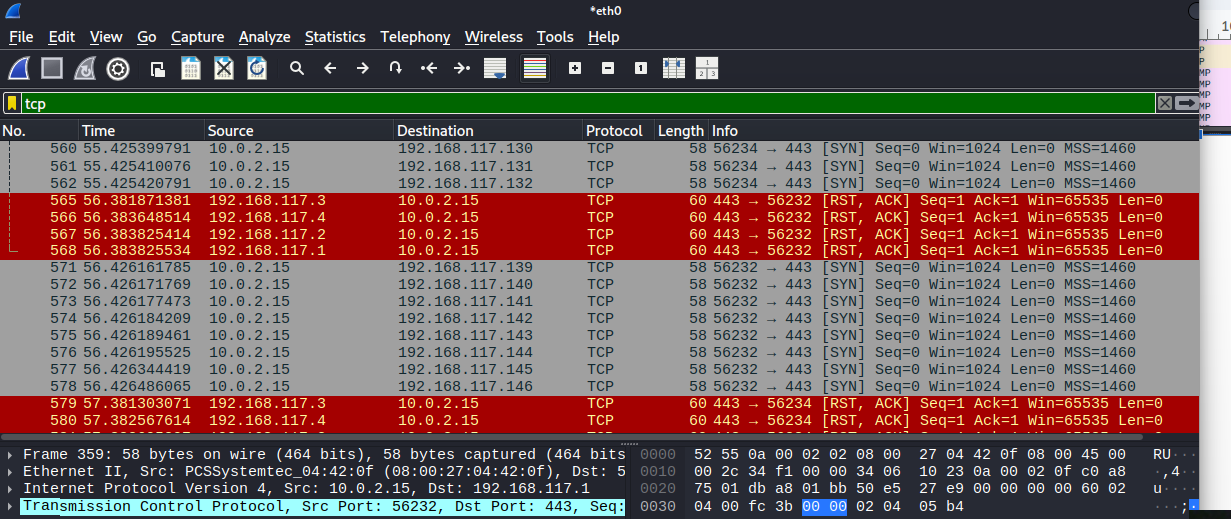
* **Bước 5** : dừng bắt gói tin trong Wireshark.

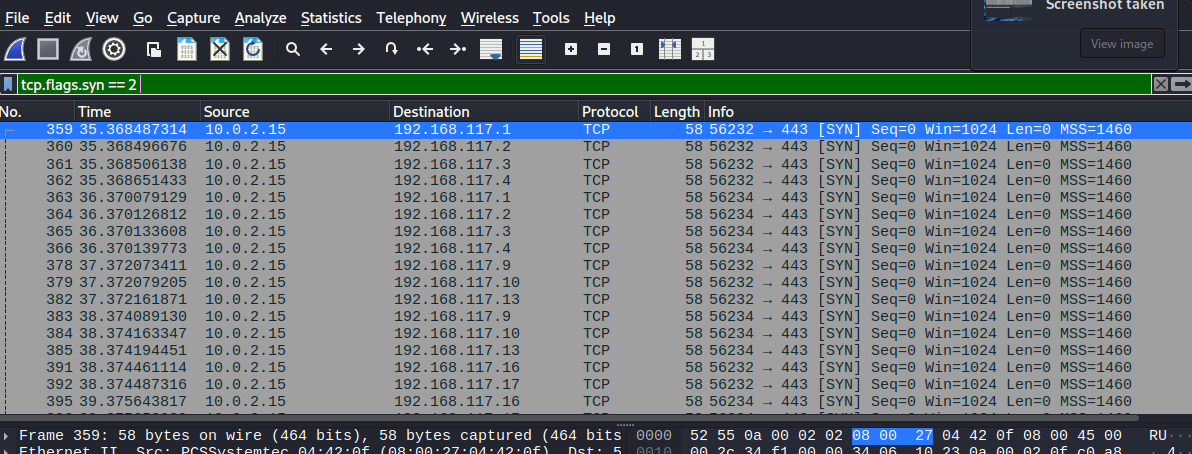
**Phân tích lưu lượng:**

- Chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. Tương tự kịch bản trên, có thể thấy rằng máy tấn công đang gửi đi một loạt các gói tin ARP Request để tìm kiếm địa chỉ MAC của các máy tính trong mạng 192.168.117.0/24

**

- Nhập giá trị **tcp** vào bộ lọc. Trên kết quả phân tích lưu lượng của Wireshark chúng ta có thể thấy gói tin TCP RST/ACK được gửi từ cổng

**



**=> Kết quả**: Như vậy, trong kịch bản vừa thực hiện, Nmap đã sử dụng kỹ thuật ARP Ping Scan và TCP SYN Scan để phát hiện các nút mạng cung cấp dịch vụ.

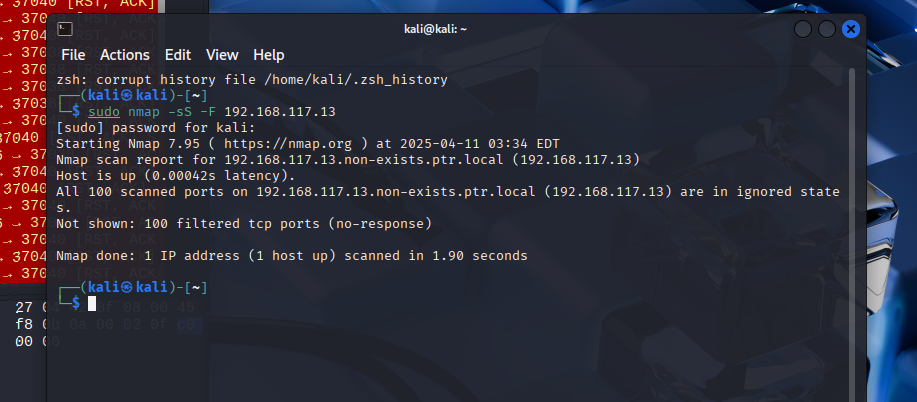
* 1. **Kịch bản 3: Quet cổng dịch vụ**
* Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm
* Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm

- **Bước 1:** Truy cập máy ảo Attack

- **Bước 2:** Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin. - **Bước 3:** Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

**nmap -sT 192.168.117.13**

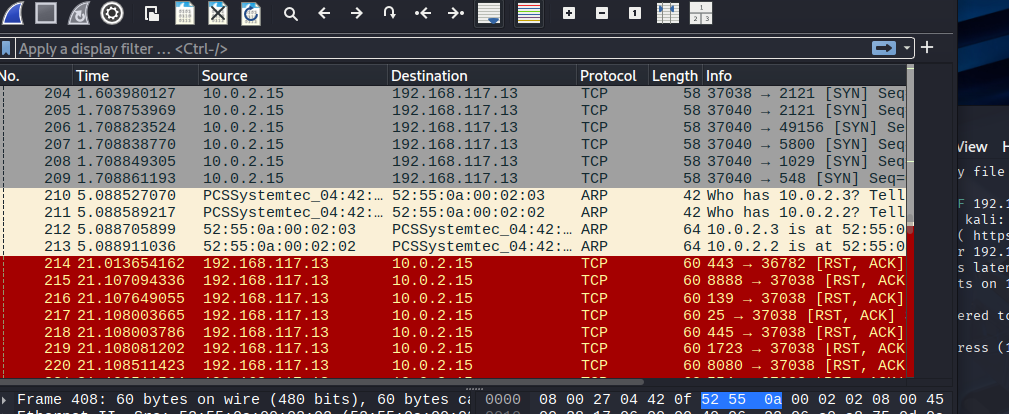
- **Bước 4:** Sau khi nmap thực hiện xong quá trình quét mạng, ta có kết quả tương tự như dưới đây. Kết quả cho thấy các cổng dịch vụ 22, 23, 53 trên máy mục tiêu 192.168.117.13 có trạng thái open. Ta có thể phán đoán máy này đang cung cấp các dịch vụ tương ứng là ssh, telnet và dns.

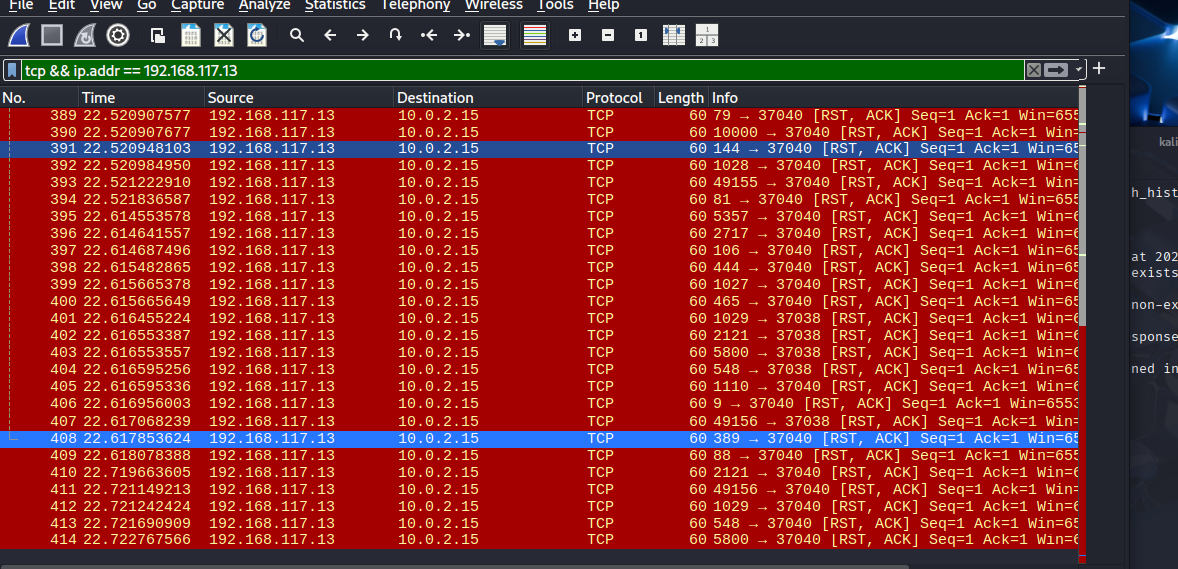
**

**Phân tích lưu lượng:**

- Quan sát file lưu lượng ta thấy trước tiên máy tấn công gửi gói tin ARP Request để kiểm tra máy mục tiêu 192.168.117.13 có hoạt động hay không. Sau đó, ta thấy một lượng lớn các gói

tin TCP SYN được gửi từ máy tấn công (192.168.117.10) tới máy mục tiêu là 192.168.117.13. Các gói tin SYN này được gửi tới các cổng ứng dụng khác nhau.

**

**

1. **Thu thập thông tin hệ thống**

* Hãy cho biết lệnh quét thăm dò tìm kiếm máy chủ email là gì? Giải thích các tham số sử dụng trong lệnh này?(1 điểm)

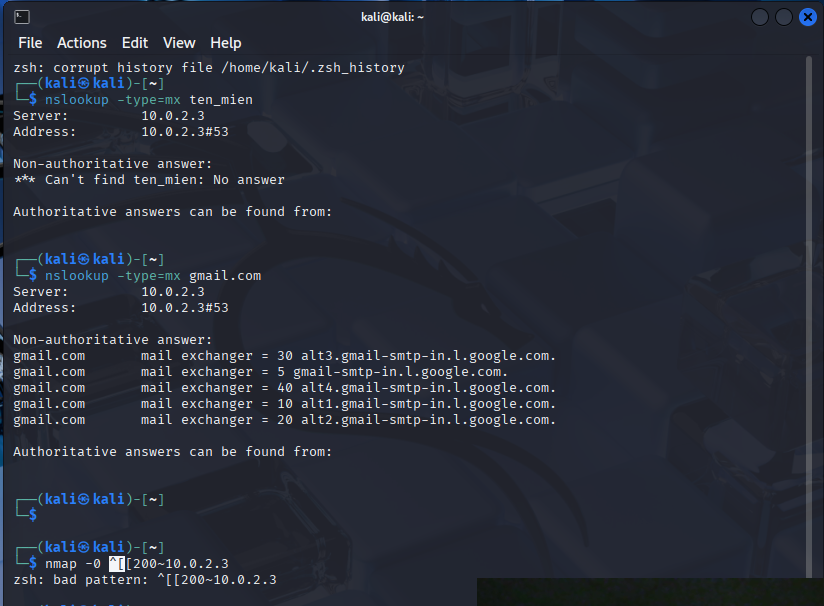
lệnh quét thăm dò: nslookup -type=mx ten\_mien

nslookup: công cụ tra cứu bản ghi Dns  
-type=mx: chỉ định truy vấn bản ghi MX

ten\_mien: là tên miền muốn tra cứu ở đây ví dụ là mail exchange

**Thông tin hệ điều hành:**

* Hình ảnh chụp kết quả của nmap: 0.25 điểm
* Nêu tên và phiên bản hệ điều hành: 0.25 điểm



**Thông tin dịch vụ: 1 điểm**

* Hình ảnh chụp kết quả của nmap: 0.25 điểm
* Danh sách dịch vụ: 0.75 điểm

| **STT** | **Tên dịch vụ** | **Số hiệu cổng ứng dụng** | **Tên phần mềm và phiên bản** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. **Tìm kiếm thông tin về các lỗ hổng**

Báo cáo ngắn gọn về các lỗ hổng đã được công bố trên các phần mềm cung cấp dịch vụ.

Mỗi lỗ hổng: 1 điểm

| **Phần mềm dịch vụ**  **(tên dịch vụ, tên phần mềm, phiên bản)** | **Số CVE** | **Mô tả ngắn gọn về lỗ hổng (Tiếng Việt)** |
| --- | --- | --- |
| SSH,OPENSSH,7.2P2 | CVE-2016-6516 | thực thi trái phép qua config lỗi |
|  |  |  |